★KELL/ P85;T01 2000-055886/05 ★FR 2778483-A1

Authentication of integrity of documents using cryptographic techniques

KELLER J 1998.05.07 1998FR-006057

T04 T05 W01 (1999.11.12) G09C 5/00, G06K 9/18, H04L 9/30

Novelty: The authentication system has a module that reads a digital or graphic seal (12) associated with each page (10) of the document or with part (11) of the text of the document. The seal can be interpreted only with a decryption key, allowing validation of the content and the sender of the document.

Use: Contracts, certificates and diplomas, patents, bank drafts and similar documents where authenticity is important.

Advantage: Allows the validation of not only the content of the document but also the authenticity of the sender, and can be applied to copies or facsimile versions of the document.

Description of Drawing(s): The drawing shows a document page marked with a bar code seal.

Page 10

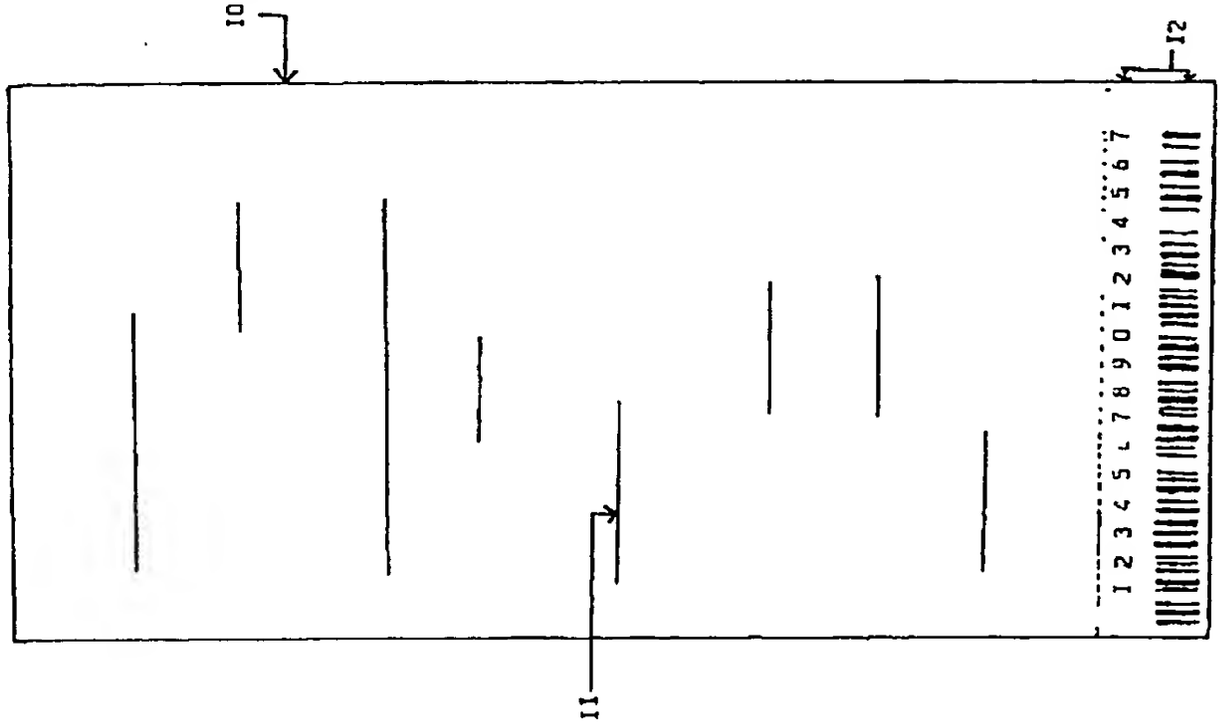
Text region 11

Seal marking 12

(9pp Dwg.No.1/2)

N2000-043681

T01-D01; T04-C02; T04-D01; T05-J; W01-A05A



A

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 778 483**

(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **98 06057**

(51) Int Cl[6] : G 09 C 5/00, H 04 L 9/30, G 06 K 9/18

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 07.05.98.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 12.11.99 Bulletin 99/45.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *KELLER JACQUES* — FR.

(72) **Inventeur(s)** : KELLER JACQUES.

(73) **Titulaire(s)** :

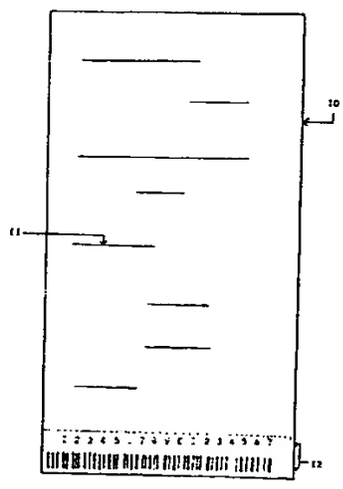
(74) **Mandataire(s)** :

(54) DISPOSITIF D'AUTHENTIFICATION ET D'INTEGRITE D'UN DOCUMENT PAR PROTECTION CRYPTOLOGIQUE.

(57) L'invention concerne un dispositif d'authentification et d'intégrité d'un document qui comprend: un module de saisie et de chiffrement qui associe à chaque page (10) d'un texte ou d'une partie de texte (11) à protéger un sceau numérique et graphique (12) dont l'interprétation n'est possible qu'avec une clé de déchiffrement;

un module de saisie et de déchiffrement permettant l'authentification de l'émetteur et l'intégrité du texte examiné.

Cette invention permet de certifier les copies d'un acte original et incessible et de les protéger contre les falsifications.



FR 2 778 483 - A1

Dispositif d'authentification et d'intégrité d'un document par protection cryptologique

L'invention concerne un dispositif d'authentification et d'intégrité d'un document par protection cryptologique.

Elle s'applique à tous documents comportant un texte dont l'authentification et l'intégrité sont jugés essentielles et capitales.

La protection de documents sur papier est une préoccupation forte des banquiers ou des distributeurs de billets en tout genre. La caractéristique de ces applications repose sur le secret de fabrication du document support. Il est, de ce fait, nécessaire de détenir l'original pour en accepter la valeur. De multiples inventions concernant la technique de fabrication de papiers spéciaux découlent directement de ce besoin. L'objectif est toujours d'éviter les falsifications.

Il existe cependant des besoins plus modestes: factures, devis, attestations de diplôme, relevés bancaires, contrats, brevets...pour lesquels le problème de la sécurité existe aussi. De plus la vie courante montre qu'il est bien souvent pratique de pouvoir utiliser une copie du document original, ne serait-ce qu'en raison de sa transmission par télécopie, par exemple. Le détenteur ne souhaite pas, en général, se dessaisir de son document original, il préfère plutôt céder autant de copies que nécessaire.

Aussi l'invention consiste à rendre les copies aussi crédibles qu'un original, ceci par le moyen donné au destinataire de pouvoir contrôler à la fois l'intégrité du texte, mais aussi, l'authenticité de l'émetteur. Cette double opération est rendue possible par l'usage de la cryptologie à clés publiques.

La figure 1 est la présentation d'une feuille authentifiée.

La figure 2 est une présentation du processus entre l'émetteur et le destinataire.

Le dispositif d'authentification et d'intégrité d'un document est caractérisé par un module de traitement qui permet de saisir le texte (11) et d'associer à chaque page (10) un sceau, objet d'un calcul, qui est lui-même placé en bas de page pour une meilleure utilisation. Selon une caractérisation préférentielle le sceau (12) est composé d'une suite numérique et d'une trame graphique représentant le code à barres de la dite suite. La partie graphique du sceau est de préférence constituée de barres étroites ou larges, espacées entre elles par une valeur plus ou moins large et représentant un code d'information numérique, par exemple: le code « 2 parmi 5 ».

Le dispositif comprend un micro-ordinateur (13) dont le programme de saisie permet, en outre, l'exécution d'un chiffrement et le placement d'un sceau en fin de page.

Le micro-ordinateur comporte, éventuellement, un lecteur de cartes à mémoire (14) capable de lire une carte à mémoire permettant de saisir les paramètres de chiffrement du sceau (clé privée et modulo de travail). Coté du destinataire, le dispositif comprend un micro-ordinateur (15) doté d'un module de saisie du texte et d'un module de déchiffrement. Il comporte éventuellement un lecteur optique (16) permettant de saisir le sceau sous sa forme de code à barres. Ceci évite le risque de lecture erronée.

La constitution du sceau fait appel à l'ensemble des caractères retenus pour être réputé intègre (tout ou partie du texte) et à une clé de chiffrement constituée en deux parties: la clé privée et le modulo de travail. L'exploitation du sceau fait appel au texte que l'on a placé en majuscules ou en soulignage (voire même l'ensemble du texte) et à une clé de chiffrement constituée de deux parties : une clé publique et un modulo de travail. Le calcul de la signature s'appuie sur le nombre de caractères du texte (caractères alpha-numériques et codes de service), sur leur transformation en un code spécifique de façon à obtenir leur somme et leur produit dans un modulo tenu secret.

L'émetteur du texte à protéger, frappe ses caractères d'une façon caractéristique de manière à ce que le destinataire puisse reprendre le même texte tapé. Plusieurs façons sont possibles : gros caractères, soulignage, ou même tout le texte. La reprise des caractères tapés est fondamentale pour une bonne interprétation, et donc, un bon contrôle.

Le texte ainsi tapé est soumis à un premier module de calcul dont l'objectif est d'obtenir une signature numérique du texte. Cette signature intègre les caractères utilisés, les signes de ponctuation et les codes de mise en forme dans la page. Un algorithme de compression spécifique permet d'obtenir un résultat numérique rigoureusement fonction du texte saisi. L'altération d'un signe ou d'un caractère donne une autre signature. Cet algorithme de compression prend en compte le nombre de caractères ou signes du texte, leur somme et leur produit. Le résultat est un train de 100 bits ou une trentaine de chiffres. Ce train est appelé « signature ». L'intégrité de la signature du document a maintenant besoin d'être chiffrée par son auteur pour en assurer l'inviolabilité. C'est l'objet du second module.

Le second module consiste à intégrer la signature dans un algorithme cryptologique à clés publiques. L'auteur du document détient une clé privée confidentielle et un modulo de travail avec lesquels le second module va générer une suite numérique inscrite en bas

de page, cette suite peut être générée sous la forme d'un code à barres pour permettre une lecture par moyen optique. L'opérateur effectuant le travail peut disposer d'un lecteur de cartes à mémoire pour conserver, bien au secret, les paramètres du chiffrement (clé privée et modulo de travail).

Pour vérifier l'authenticité tout un chacun peut s'enquérir de la clé publique de l'auteur du document, son modulo de travail et reconstituer les mêmes étapes que l'auteur. Cette opération par déchiffrement donne une signature et si il y a concordance avec celle obtenue par la saisie directe du texte, on peut alors conclure qu'il y a certitude sur l'intégrité du texte et sur l'authenticité de l'auteur. Pour que la sécurité de l'opération soit bien assurée, il faut que le canal d'obtention des paramètres de l'émetteur soit bien indépendant de celui de l'acheminement du document lui-même. En effet, si l'indépendance n'est pas assurée, une falsification du document avec un abus d'usage de la clé privée entraînerait une apparence d'intégrité et d'authentification.

Un confort technique peut être apporté à la ré-écriture du texte par le destinataire. Ce confort s'obtient par un balayage électronique du document et sa projection sur un écran cathodique. La sélection du texte se fait alors par un curseur.

Un autre confort technique réside dans la lecture du code à barres représentant la suite numérique qui sert de sceau au document, au moyen d'un lecteur optique. Cela évite les erreurs de lecture.

Enfin un dernier confort réside dans la mise en place d'un lecteur de carte à mémoire contenant les clés de chiffrement pour l'émetteur du document. Ceci évite aussi de faire une erreur de saisie et cela améliore la conservation des clés

REVENDICATIONS

1-Dispositif d'authentification et d'intégrité d'un document caractérisé par un module de traitement qui permet de saisir un texte (11) et d'associer à chaque page (10) un sceau (12).

2- Dispositif selon la revendication 1, caractérisé en ce que le sceau (12) est la traduction d'une signature numérique chiffrée obtenue à partir des éléments constitutifs du texte à protéger.

3- Dispositif selon la revendication 1, caractérisé en ce que le sceau (12) est la traduction graphique d'une information numérique, sous forme de barres épaisses ou fines, espacées entre elles par une valeur plus ou moins large et placées en fin de page.

4- Dispositif selon la revendication 1, caractérisé en ce que le dispositif comprend un micro-ordinateur (13) dont le programme de saisie permet, en outre, l'exécution d'un chiffrement et le placement d'un sceau en fin de page.

5- Dispositif selon la revendication 4, caractérisé en ce que le micro-ordinateur comporte, éventuellement, un lecteur de cartes à mémoire (14) capable de lire une carte à mémoire permettant de saisir les paramètres de chiffrement du sceau (clé privée et modulo de travail).

6- Dispositif selon la revendication 1, caractérisé en ce que, du coté du destinataire, il comprend un micro-ordinateur (15) doté d'un module de saisie du texte et d'un module de déchiffrement.

7- Dispositif selon la revendication 6, caractérisé en ce que le micro-ordinateur comporte éventuellement un lecteur optique (16) permettant de saisir le sceau sous une forme de code à barres.

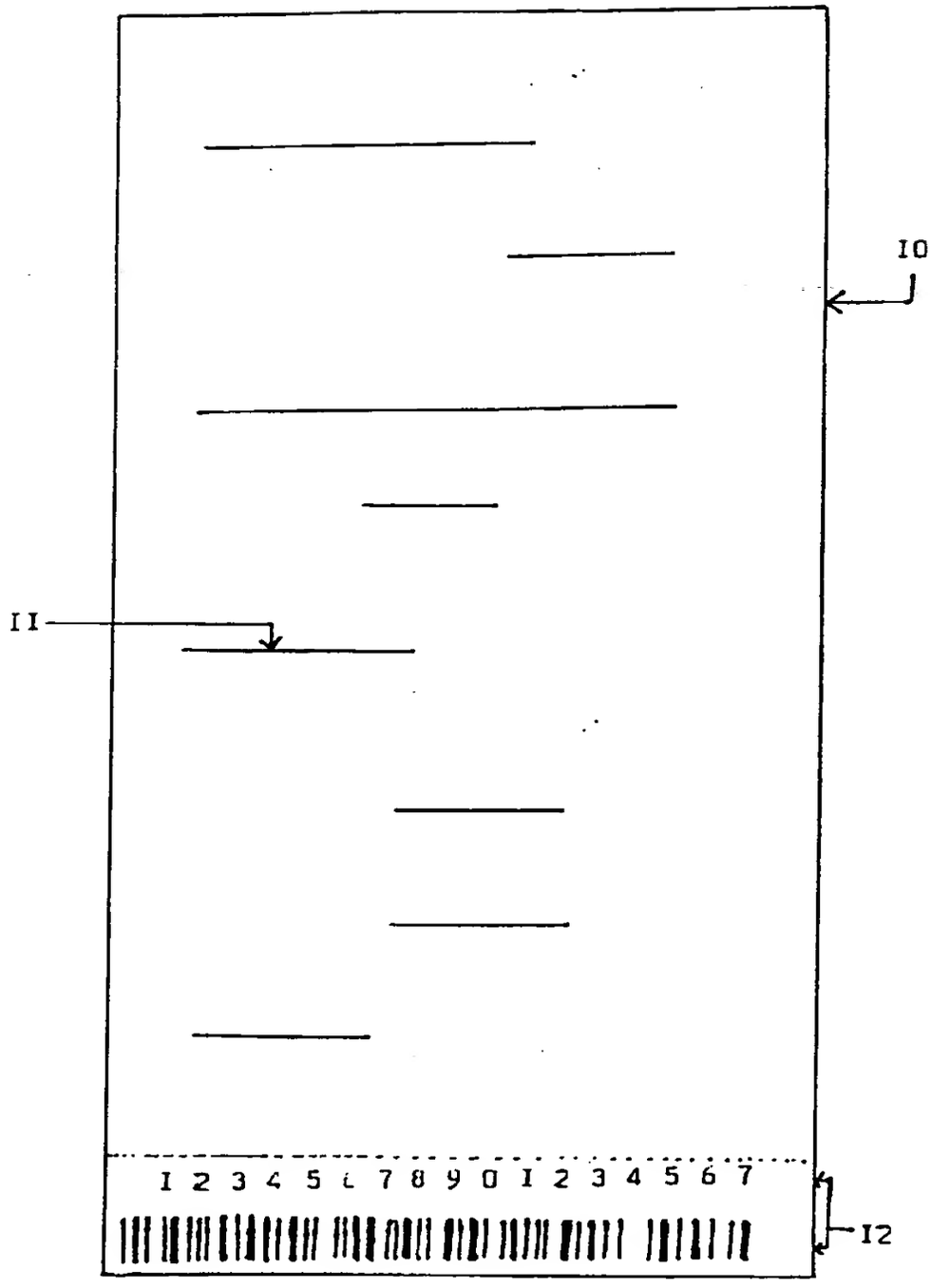
8- Procédé destiné à la mise en œuvre du dispositif selon la revendication 2, caractérisé en ce que le calcul de la signature numérique s'appuie sur l'ensemble des caractères du texte protégé (caractères alpha-numériques et codes de service), en tenant compte de leur nombre, leur somme et leur produit dans un modulo tenu secret.

9- Procédé destiné à la mise en œuvre du dispositif selon la revendication 4, caractérisé en ce que la constitution de la signature numérique fait appel à l'ensemble des caractères à protéger (tout ou partie du texte) et à un chiffrement de cette dernière permettant d'obtenir un sceau à partir d'une clé constituée en deux parties: la clé privée et le modulo de travail

10- Procédé destiné à la mise en œuvre du dispositif selon la revendication 6, caractérisé en ce que le sceau fait l'objet d'un déchiffrement à partir de la clé publique et du modulo de travail, afin d'obtenir la signature numérique qui est comparée ensuite à celle obtenue directement à partir de l'ensemble des caractères protégées.

5

PLANCHE I/2



FigureI

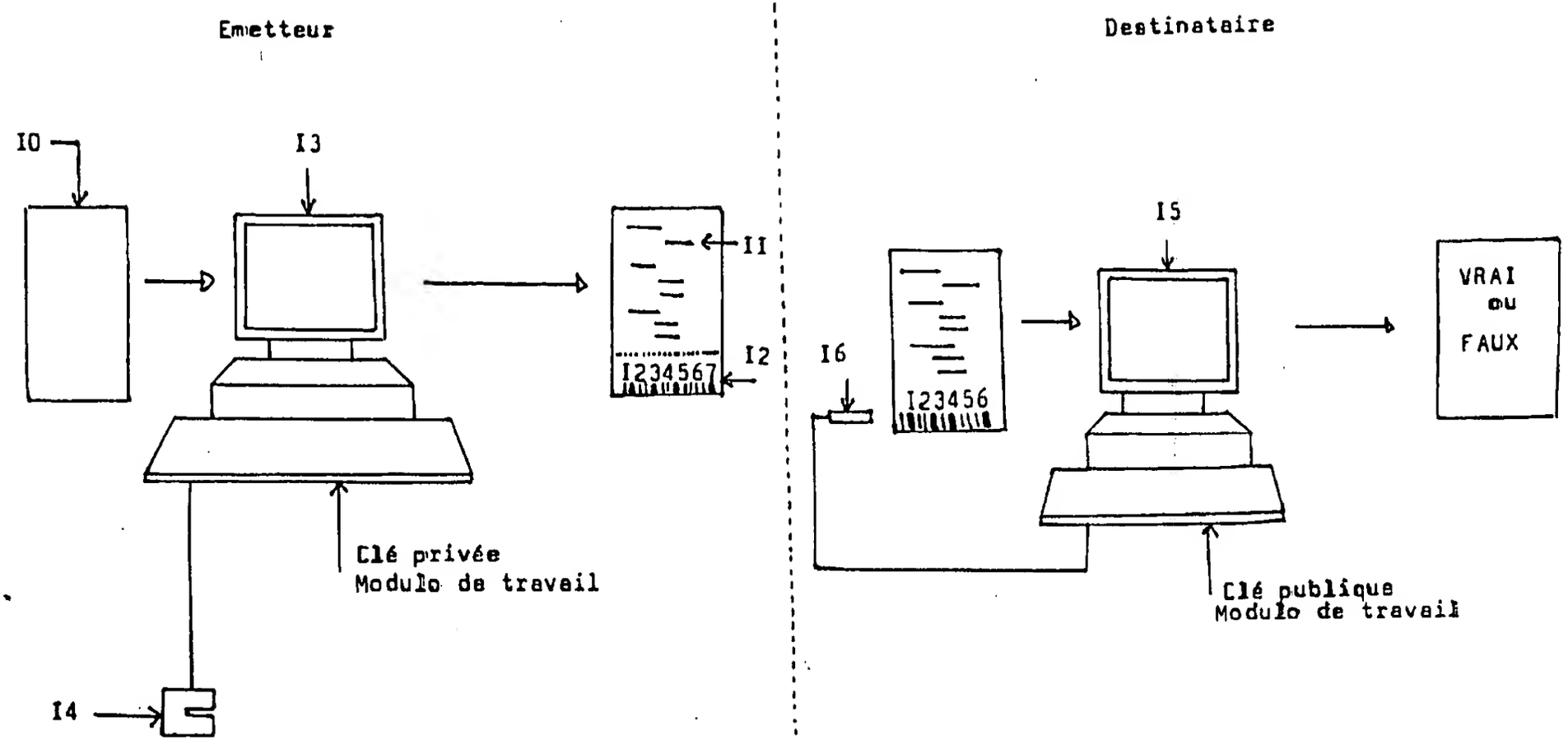


Figure II

PLANCHE 2/2

2778483

2778483

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 560352
FR 9806057

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X Y	EP 0 547 837 A (XEROX CORP) 23 juin 1993 * revendication 1; figure 1A *	1,2,4-6, 8-10 3,7
Y	US 4 463 250 A (MCNEIGHT DAVID L ET AL) 31 juillet 1984 * revendication 1; figure 2 *	3,7
A	EP 0 782 114 A (IBM) 2 juillet 1997 * revendication 1; figure 1 *	1-10
A	US 4 179 212 A (LAHR ROY J) 18 décembre 1979 * revendication 1; figure 1 *	1-10
A	US 4 649 266 A (ECKERT ALTON B) 10 mars 1987 * revendication 1; figure 1 *	1-10
A	WO 80 02757 A (WINDERLICH H ;STOCKBURGER H (DE)) 11 décembre 1980 * revendication 1; figure 1A *	1-10

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G07D
G07F

Date d'achèvement de la recherche: 20 janvier 1999

Examinateur: Kirsten, K

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

1